Implementing and Operating Cisco Security Core Technologies

Référence : **SCOR** Durée : **5 jours** Certification : **350-701**

CONNAISSANCES PREALABLES

• 1-Familiarity with Ethernet and TCP/IP networking. • 2-Working Knowledge of the Windows operating system. • 3-Working Knowledge of Cisco IOS networking and concepts. • 4-Familiarity with basics of networking security concepts.

PROFIL DES STAGIAIRES

• Security engineer ; Network engineer ; Network designer ; Network administrator ; Systems engineer ; Consulting systems engineer ; Technical solutions architect ; Network manager ; Cisco integrators and partners.

OBJECTIFS

• Describe information security concepts and strategies within the network. • Describe common TCP/IP, network application, and endpoint attacks. • Describe how various network security technologies work together to guard against attacks. • Implement access control on Cisco ASA appliance and Cisco Firepower Next-Generation Firewall. • Describe and implement basic email content security features and functions provided by Cisco Email Security Appliance. • Describe and implement web content security features and functions provided by Cisco Web Security Appliance. • Describe Cisco Umbrella security capabilities, deployment models, policy management, and Investigate console. • Introduce VPNs and describe cryptography solutions and algorithms. • Describe Cisco secure site-to-site connectivity solutions and explain how to deploy Cisco IOS VTI-based point-to-point IPsec VPNs, and point-to-point IPsec VPN on the Cisco ASA and Cisco FirePower NGFW. • Describe and deploy Cisco secure remote access connectivity solutions and describe how to configure 802.1X and EAP authentication. • Provide basic understanding of endpoint security and describe AMP for Endpoints architecture and basic features. • Examine various defenses on Cisco devices that protect the control and management plane. • Configure and verify Cisco IOS Software Layer 2 and Layer 3 Data Plane Controls. • Describe Cisco Stealthwatch Enterprise and Stealthwatch Cloud solutions. • Describe basics of cloud computing and common cloud attacks and how to secure cloud environment.

CERTIFICATION PREPAREE

Implementing and Operating Cisco Security Core Technologies (SCOR 350-701). This is the core exam for the Cisco CCNP Security certification, in order to gain the CCNP Security certification you will also need to pass one of the concentration exams

METHODES PEDAGOGIQUES

- Mise à disposition d'un poste de travail par stagiaire
- Remise d'une documentation pédagogique papier ou numérique pendant le stage
- La formation est constituée d'apports théoriques, d'exercices pratiques, de réflexions et de retours d'expérience
- Le suivi de cette formation donne lieu à la signature d'une feuille d'émargement

FORMATEUR

Consultant-Formateur expert Security Cisco

METHODE D'EVALUATION DES ACQUIS

- Auto-évaluation des acquis par le stagiaire via un questionnaire
- Attestation de fin de stage adressée avec la facture

CONTENU DU COURS

Describing Information Security Concepts*

Describing Common TCP/IP Attacks*

Describing Common Network Application Attacks*

Describing Common Endpoint Attacks*

Describing Network Security Technologies

- Defense-in-Depth Strategy
- Defending Across the Attack Continuum
- Network Segmentation and Virtualization Overview
- Stateful Firewall Overview
- Security Intelligence Overview
- Threat Information Standardization
- Network-Based Malware Protection Overview
- Intrusion Prevention System (IPS) Overview
- Next Generation Firewall Overview
- Email Content Security Overview
- Web Content Security Overview
- Threat Analytic Systems Overview
- DNS Security Overview
- Authentication, Authorization, and Accounting Overview
- Identity and Access Management Overview
- Virtual Private Network Technology Overview
- Network Security Device Form Factors Overview

Deploying Cisco ASA Firewall

- Cisco ASA Deployment Types
- Cisco ASA Interface Security Levels
- Cisco ASA Objects and Object Groups
- Network Address Translation
- Cisco ASA Interface Access Control Lists (ACLs)
- Cisco ASA Global ACLs
- Cisco ASA Advanced Access Policies
- Cisco ASA High Availability Overview

Deploying Cisco Firepower Next-Generation Firewall

- Cisco Firepower NGFW Deployments
- Cisco Firepower NGFW Packet Processing and Policies
- Cisco Firepower NGFW Objects
- Cisco Firepower NGFW Network Address Translation (NAT)
- Cisco Firepower NGFW Prefilter Policies
- Cisco Firepower NGFW Access Control Policies
- Cisco Firepower NGFW Security Intelligence
- Cisco Firepower NGFW Discovery Policies
- Cisco Firepower NGFW IPS Policies
- Cisco Firepower NGFW Malware and File Policies

Deploying Email Content Security

- Cisco Email Content Security Overview
- Simple Mail Transfer Protocol (SMTP) Overview
- Email Pipeline Overview
- Public and Private Listeners
- Host Access Table Overview
- Recipient Access Table Overview
- Mail Policies Overview
- Protection Against Spam and Graymail
- Anti-virus and Anti-malware Protection
- Outbreak Filters
- Content Filters
- Data Loss Prevention
- Email Encryption

Deploying Web Content Security

- Cisco Web Security Appliance (WSA) Overview
- Deployment Options
- Network Users Authentication
- Secure HTTP (HTTPS) Traffic Decryption
- Access Policies and Identification Profiles
- Acceptable Use Controls Settings
- Anti-Malware Protection

Deploying Cisco Umbrella*

Explaining VPN Technologies and Cryptography

- VPN Definition
- VPN Types
- Secure Communication and Cryptographic Services
- Keys in Cryptography
- Public Key Infrastructure

Introducing Cisco Secure Site-to-Site VPN Solutions

- Site-to-Site VPN Topologies
- IPsec VPN Overview
- IPsec Static Crypto Maps
- IPsec Static Virtual Tunnel Interface
- Dynamic Multipoint VPN
- Cisco IOS FlexVPN

Deploying Cisco IOS VTI-Based Point-to-Point IPsec VPNs

- Cisco IOS VTIs
- Static VTI Point-to-Point IPsec Internet Key Exchange (IKE) v2 VPN Configuration

Deploying Point-to-Point IPsec VPNs on the Cisco ASA and Cisco Firepower NGFW

- Point-to-Point VPNs on the Cisco ASA and Cisco Firepower NGFW
- Cisco ASA Point-to-Point VPN Configuration
- Cisco Firepower NGFW Point-to-Point VPN Configuration

Introducing Cisco Secure Remote Access VPN Solutions

- Remote Access VPN Components
- Remote Access VPN Technologies
- Secure Sockets Layer (SSL) Overview

Deploying Remote Access SSL VPNs on the Cisco ASA and Cisco Firepower NGFW

- Remote Access Configuration Concepts
- Connection Profiles
- Group Policies
- Cisco ASA Remote Access VPN Configuration
- Cisco Firepower NGFW Remote Access VPN Configuration

Explaining Cisco Secure Network Access Solutions

- Cisco Secure Network Access
- Cisco Secure Network Access Components
- AAA Role in Cisco Secure Network Access Solution
- Cisco Identity Services Engine
- Cisco TrustSec

Describing 802.1X Authentication

- 802.1X and Extensible Authentication Protocol (EAP)
- EAP Methods
- Role of Remote Authentication Dial-in User Service (RADIUS) in 802.1X Communications
- RADIUS Change of Authorization

Configuring 802.1X Authentication

- Cisco Catalyst® Switch 802.1X Configuration
- Cisco Wireless LAN Controller (WLC) 802.1X Configuration
- Cisco Identity Services Engine (ISE) 802.1X Configuration
- Supplicant 802.1x Configuration
- Cisco Central Web Authentication

Describing Endpoint Security Technologies*

Deploying Cisco Advanced Malware Protection (AMP) for Endpoints*

Introducing Network Infrastructure Protection*

Deploying Control Plane Security Controls*

Deploying Layer 2 Data Plane Security Controls*

Deploying Layer 3 Data Plane Security Controls*

Deploying Management Plane Security Controls*

Deploying Traffic Telemetry Methods*

Deploying Cisco Stealthwatch Enterprise*

Describing Cloud and Common Cloud Attacks*

Securing the Cloud*

Deploying Cisco Stealthwatch Cloud*

Describing Software-Defined Networking (SDN*)*

Labs

- Configure Network Settings and NAT on Cisco ASA
- Configure Cisco ASA Access Control Policies
- Configure Cisco Firepower NGFW NAT
- Configure Cisco Firepower NGFW Access Control Policy
- Configure Cisco Firepower NGFW Discovery and IPS Policy
- Configure Cisco NGFW Malware and File Policy
- Configure Listener, Host Access Table (HAT), and Recipient Access Table (RAT) on Cisco Email Security Appliance (ESA)
- Configure Mail Policies
- Configure Proxy Services, Authentication, and HTTPS Decryption
- Enforce Acceptable Use Control and Malware Protection
- Examine the Umbrella Dashboard
- Examine Cisco Umbrella Investigate
- Explore DNS Ransomware Protection by Cisco Umbrella
- Configure Static VTI Point-to-Point IPsec IKEv2 Tunnel
- Configure Point-to-Point VPN between the Cisco ASA and Cisco Firepower NGFW
- Configure Remote Access VPN on the Cisco Firepower NGFW
- Explore Cisco AMP for Endpoints
- Perform Endpoint Analysis Using AMP for Endpoints Console
- Explore File Ransomware Protection by Cisco AMP for Endpoints Console
- Explore Cisco Stealthwatch Enterprise v6.9.3
- Explore Cognitive Threat Analytics (CTA) in Stealthwatch Enterprise v7.0
- Explore the Cisco Cloudlock Dashboard and User Security
- Explore Cisco Cloudlock Application and Data Security
- Explore Cisco Stealthwatch Cloud
- Explore Stealthwatch Cloud Alert Settings, Watchlists, and Sensors

** This section is self-study material that can be done at your own pace if you are taking the instructor-led version of this course*

Certification CISCO Implementing and Operating Cisco Security Core Technologies

- Cette formation prépare au passage de la certification Implementing and Operating Cisco Security Core Technologies